UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,908	05/16/2005	Bernd Meyer	30691/DP018	6775

4743 7590 11/24/2006

MARSHALL, GERSTEIN & BORUN LLP
233 S. WACKER DRIVE, SUITE 6300
SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
DOAN, TRANG T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/506,908	**Applicant(s)** MEYER ET AL.	
	Examiner Trang Doan	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☒ Claim(s) *1 and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03/16/2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *09/2004*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 are pending in this application.

Claim Objections

2. Regarding claim 1, a transaction indicator, in line 7, is the same as a transaction indicator, in line 3, or they are different. Appropriate correction is required.

3. Regarding claim 1, the functionality of an intermediate station, in line 12, does not do anything except for storing information, therefore the examiner interprets the contact station and the intermediate station as one unit.

4. Claim 17 is objected to because of the following informalities: claim 17 depends on claim 19, however lowering claim cannot depend on highering claim. Appropriate correction is required.

Drawings

5. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the amendment document filed on 07/18/2005 is considered no-compliant because it has failed to meet the requirement of 37 CFR 1.121. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Regarding claim 5, "the producer entering his own data into the cryptographic module" , in lines 4, is not clear to the examiner. The step of entering data does not recite in claim 1 and further what type of "data" is it. Appropriate correction is required.

9. Regarding claim 6, "linking the data entered by the document producer to the key information by means of cryptographic module" is confused to the examiner. Examiner interprets linking the data entered by producer to the key information as combining these two data types in the cryptographic module to produce an output. However, linking method needs to be more precise cause the examiner does not understand how the cryptographic module links these two data types together. Appropriate correction is required.

10. Regarding claim 7, the examiner does not understand how the linking method works by using data entered by producer, decrypted key information and key information. Appropriate correction is required.

11. Regarding claims 8, 15 and 19-22, the examiner needs a clarification on these claims. Appropriate correction is required.

12. Claims 16-17 recite the limitation "the two types of data" in lines 1 and 3. There is insufficient antecedent basis for this limitation in the claim.

13. The claims 1-24 are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors. Appropriate correction is required.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 1-15 and 23-24 are rejected under 35 U.S.C. 102(b) as being anticipated by Rowney et al. (US 5987140) (hereinafter Row).

16. Regarding claim 1, Row teaches the steps of generating random key information and forming encrypted checking information from the key information and from a transaction indicator in a cryptographically reliable contact station (Row: see figure 4 and column 13 lines 4-20: Merchant generates a random encryption key and then uses the random encryption key to encrypt combined block (530: comprises authorization request, public key certificate, signature public key certificate and digital signature) to form encrypted combined block (550)), encrypting the key information in the cryptographically reliable contact station (Row: column 13 lines 21-24), transmitting the

encrypted checking information and the encrypted key information by the cryptographically reliable contact station to an intermediate station (Row: column 13 lines 29-36), the intermediate station temporarily storing the encrypted key information and the encrypted checking information and subsequently transmitting this to a cryptographic module of a document producer at a different point in time from the transfer between the cryptographically reliable contact station and the intermediate station (Row: see figure 1C).

17. Regarding claim 2, Row teaches generating the key information in such a way that the key information is formed randomly (Row: column 13 lines 4-14).

18. Regarding claim 3, Row teaches configuring at least one of the encrypted key information and the encrypted checking information is in such a way that it cannot be decrypted in the intermediate station (Row: column 16 lines 10-22).

19. Regarding claim 4, Row teaches the cryptographic module decrypting the key information with a key contained in the cryptographic module (Row: column 13 lines 45-58).

20. Regarding claim 5, Row teaches the document producer entering his own data into the cryptographic module (Row: column 14 lines 1-13).

21. Regarding claim 6, Row teaches irreversibly linking the data entered by the document producer to the key information by means of the cryptographic module (Row: see figures 6 A and B).

22. Regarding claim 7, Row teaches irreversibly linking the data entered by the document producer and the decrypted key information by using the key information to form a check value for the document (Row: column 12 lines 43-65).

23. Regarding claim 8, Row teaches forming at least one of a document and a data record from the result of the irreversible linking of the data entered by the document producer with the decrypted key information and transmitting the document or data record to a checking station (Row: see figures 6 A and B).

24. Regarding claim 9, Row teaches wherein the document or data record transmitted to the checking station contains the document producer's own data, at least partially in plain text (Row: see figures 6 A and B).

25. Regarding claim 10, Row teaches entering the encrypted checking information into the document or data record that is transmitted to the checking station (Row: see figures 6 A and B).

26. Regarding claim 11, Row teaches encrypting information remaining in the cryptographic module in such a way that it can be decrypted in the cryptographic module (Row: see figure 8).

27. Regarding claim 12, Row teaches supplying the cryptographic module with the information, also in case of a supply via communication partners that are not reliable in the cryptographic sense, by a cryptographically reliable station whose information can be relied on by the checking station (Row: see figure 12 and column 17 lines 44-67 and column 18 lines 1-33).

28. Regarding claim 13, Row teaches in order for a reliable station to provide reliable information for the cryptographic module, using cryptographic encryptions that the checking station can reverse (Row: column 13 lines 4-13).

29. Regarding claim 14, Row teaches supplying the cryptographic module via communication partners that are cryptographically non-reliable in such a way that the information is forwarded to the cryptographic module at a different point in time (Row: see figure 1C and column 18 lines 34-42).

30. Regarding claim 15, Row teaches supplying of the cryptographic module via communication partners that are cryptographically not reliable is carried out in such a way that an exchange of information within a dialog is not necessary (Row: see figure 1B).

31. Regarding claim 23, Row teaches an interface to receive encrypted information of a cryptographically reliable contact station and to temporarily store the received encrypted information as well as means for receiving value transfer requests by at least one cryptographic module and of forwarding the received encrypted information to the cryptographic module at a different point in time (Row: see figure 1C and column 13 lines 29-36).

32. Regarding claim 24, Row teaches wherein the information is encrypted in such a way that it cannot be decrypted in the value transfer center (Row: column 16 lines 10-22).

Claim Rejections - 35 USC § 103

33. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

34. Claims 16-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Row in view of Singer (US 6724894) (hereinafter Singer).

35. Regarding claim 16, Row does not explicitly disclose cryptographically linking the two types of data to each other, such that said linking cannot be discovered by means of crypto-analysis. Singer discloses cryptographically linking the two types of data to each other, such that said linking cannot be discovered by means of crypto-analysis (Singer: see Abstract and column 3 lines 45-62). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of crypto-analysis of Singer to Row's method to reduce side channel attacks pose a significant threat to cryptographic system. Differential power analysis attacks allow an attacker to extract secret protected information from a supposedly secure cryptographic device by measuring variations in power consumption over time, and then applying sophisticated analysis to this information (Singer: column 1 lines 33-36).

36. Regarding claim 17, Row in view of Singer discloses wherein the cryptographic linking of the two types of data is such that non-linear fractions are added that are known only to the reliable contact station and to the checking station (Row: see figure 6 A and B).

37. Regarding claim 18, Row does not explicitly disclose wherein the generated forgery-proof documents or data records contain monetary value information. Singer discloses wherein the generated forgery-proof documents or data records contain monetary value information (Singer: column 3 lines 7-25). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of encrypted postage value of Singer to Row's method to generate secure postal indicia by selected data on the mailpiece as the postage value and then uses a secret key to encrypt the postage value to form an encrypted postage value.

38. Regarding claim 19, Row does not explicitly disclose connecting the monetary value information to the document or data record in such a way that a check value can be formed by comparing the monetary value information to the document or data record. Singer discloses connecting the monetary value information to the document or data record in such a way that a check value can be formed by comparing the monetary value information to the document or data record (Singer: column 7 lines 43-49). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of hash value of Singer to Row's method to create a check value (or hash value) based upon the monetary value to verify that the monetary value has not been altered because altering the monetary value would change the check value (or the hash value).

39. Regarding claim 20, Row does not explicitly disclose wherein the monetary value information contains proof of the payment of postage amounts. Singer discloses wherein the monetary value information contains proof of the payment of postage

amounts (Singer: column 9 lines 5-9 and column 10 lines 3-19 and column 3 lines 7-25). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of hash value of Singer to Row's method to create a check value (or hash value) based upon the monetary value to verify that the monetary value has not been altered because altering the monetary value would change the check value (or the hash value).

40. Regarding claim 21, Row does not explicitly disclose linking the monetary value information that proves the payment of postage amounts to identification data of the document producer. Singer discloses linking the monetary value information that proves the payment of postage amounts to identification data of the document producer (Singer: column 4 lines 23-43). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of hash value of Singer to Row's method to create a check value (or hash value) based upon the monetary value to verify that the monetary value has not been altered because altering the monetary value would change the check value (or the hash value).

41. Regarding claim 22, Row does not explicitly disclose linking the monetary value information to address data. Singer discloses linking the monetary value information to address data (Singer: column 4 lines 44-65). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of linking the postage value to address data of Singer to Row's method depending on the verification strategy additional elements, including delivery address information, may be included. An indicium should, at a minimum, contain: 1) the security data, and 2) the digital token produced by a

encryption of the security data. Cryptographic authentication proves integrity of these elements (Singer: column 4 lines 37-43).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Trang Doan
Examiner
Art Unit 2131

T.D.
11/17/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100